日　本　国　特　許　庁
JAPAN　PATENT　OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application:　２００２年１１月　７日

出願番号
Application Number:　特願２００２－３２３７９４

[ST.10/C]:　[ＪＰ２００２－３２３７９４]

出願人
Applicant(s):　新潟大学長

２００３年　１月２８日

特許庁長官
Commissioner,
Japan Patent Office　太田信一郎

出証番号　出証特２００３－３００２０９３

【書類名】　特許願
【整理番号】　U2002P113
【提出日】　平成14年11月 7日
【あて先】　特許庁長官　太田　信一郎　殿
【国際特許分類】　G06F　7/56
【発明の名称】　乱数発生方法及び乱数発生装置
【請求項の数】　10
【発明者】
【住所又は居所】　新潟県新潟市五十嵐一の町７７９４番地２０
【氏名】　斉藤　義明
【特許出願人】
【識別番号】　596133441
【氏名又は名称】　新潟大学長　長谷川　　彰
【代理人】
【識別番号】　100072051
【弁理士】
【氏名又は名称】　杉村　興作
【選任した代理人】
【識別番号】　100059258
【弁理士】
【氏名又は名称】　杉村　暁秀
【先の出願に基づく優先権主張】
【出願番号】　特願2002-221194
【出願日】　平成14年 7月30日
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9812710

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　乱数発生方法及び乱数発生装置

【特許請求の範囲】

【請求項１】　所定の電気的信号を発振した後、定常状態になるまでの立上り期間内において、前記電気的信号の振幅に対して所定の閾値を設定し、前記振幅の前記閾値に対する大小関係から０又は１の数字を割り当て、２進数的な乱数を発生させることを特徴とする、乱数発生方法。

【請求項２】　前記電気的信号は所定の発振回路から発振することを特徴とする、請求項１に記載の乱数発生方法。

【請求項３】　前記発振回路に対して所定のスイッチング回路より矩形波を入力するようにしたことを特徴とする、請求項２に記載の乱数発生方法。

【請求項４】　前記電気的信号は、前記発振回路より発振された後、所定のＡ／Ｄ変換器により、ディジタル成分に変換することを特徴とする、請求項２又は３に記載の乱数発生方法。

【請求項５】　前記電気的信号の周波数がサンプリング周波数よりも高いことを特徴とする、請求項４に記載の乱数発生方法。

【請求項６】　所定の電気的信号を発振するための発振手段と、

前記電気的信号の振幅に対して所定の閾値を設定し、前記振幅の前記閾値に対する大小関係から０又は１の数字を割り当てる演算処理手段とを具えることを特徴とする、乱数発生装置。

【請求項７】　前記発振手段は所定の発振回路を含むことを特徴とする、請求項６に記載の乱数発生装置。

【請求項８】　前記発振手段の前方において、矩形波生成手段を具えることを特徴とする、請求項６又は７に記載の乱数発生装置。

【請求項９】　前記矩形波生成手段はスイッチング回路を含むことを特徴とする、請求項８に記載の乱数発生装置。

【請求項１０】　前記発振手段と前記演算処理手段との間において、Ａ／Ｄ変換器を具えることを特徴とする、請求項６～９のいずれか一に記載の乱数発生装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、暗号作製技術などの情報産業分野、特に将来の量子コンピュータなどの分野において好適に用いることのできる乱数発生方法及び乱数発生装置に関する。

【０００２】

【従来の技術】

完全に無秩序であり、かつ全体としては出現頻度が等しくなる乱数は、社会現象や物理現象の数値シュミレーションなどに広く利用されている。また、乱数は暗号技術としても重要な役割を果たしており、情報の保護の分野でもその需要が高い。現在、乱数の発生方法として種々の方法が開発されているが、そのほとんどはアルゴリズムによるソフト的な疑似乱数の生成である。

【０００３】

アルゴリズムによる乱数生成は、ある程度の信頼性を有し、高速に乱数生成を行なうことができるという点から広く利用されている。しかしながら、コンピュータは有限の情報しかとらないために、生成された乱数は周期性を持つことが確認されている。そのため、正確な解や十分なセキュリティが得られない場合があり、より無秩序な乱数発生方法の確立が望まれている。

【０００４】

近年、ハードウエアの発展に伴う処理速度の向上と信頼性の向上から、物理的な乱数の生成方法が開発されてきた。例えば、熱電子雑音や放射性物質の崩壊などの物理現象に基づいて生成された乱数は、予測不可能性の高い、理想的な乱数列であることが知られている。しかしながら、これらの方法では高価で大掛かりな装置を必要とすることが多い。

【０００５】

【発明が解決しようとする課題】

本発明は、廉価かつ簡易な構成の装置を用いて、より無秩序な乱数を発生させる新規な方法、並びに前記方法に適用する装置を提供することを目的とする。

【０００６】

【課題を解決するための手段】

上記目的を達成すべく、本発明は、所定の電気的信号を発振した後、定常状態になるまでの立上り期間内において、前記電気的信号の振幅に対して所定の閾値を設定し、前記振幅の前記閾値に対する大小関係から０又は１の数字を割り当て、２進数的な乱数を発生させることを特徴とする、乱数発生方法に関する。

【０００７】

また、本発明は、所定の電気的信号を発振するための発振手段と、
前記電気的信号の振幅に対して所定の閾値を設定し、前記振幅の前記閾値に対する大小関係から０又は１の数字を割り当てる演算処理手段とを具えることを特徴とする、乱数発生装置に関する。

【０００８】

図１は、本発明の乱数発生方法の原理を説明するための図である。電気的信号が所定の周波数で発振されると、図１に示すように、所定の立上り期間内においては、発振回路などのランダムな雑音などの影響を受けることによって周波数及び振幅が不安定となり、前記立上り期間経過後の定常状態において、前記電気的信号は安定した周波数及び振幅で発振されるようになる。したがって、前記立上り期間内の電気的信号の振幅に対して所定の閾値を設定し、前記振幅の前記閾値に対する大小関係を通じて０又は１の数字を割り当てることによって、２進数的な乱数を発生させることができることを見出し、本発明をするに至ったものである。

【０００９】

例えば、前記閾値よりも大きな振幅に対しては１を割り当て、前記閾値よりも小さな振幅に対しては０を割り当てることによって、２進数的な乱数を発生させることができる。

【００１０】

すなわち、本発明によれば、少なくとも所定の電気的信号を発振するための発振手段と、前記電気的信号の振幅に対して所定の閾値を設定し、前記振幅の前記閾値に対する大小関係から０又は１の数字を割り当てる演算処理手段とを具える

廉価かつ簡易な装置を用いるのみで、無秩序な２進数的な乱数を発生することができるものである。

【００１１】

【発明の実施の形態】

以下、本発明を発明の実施の形態に基づいて詳細に説明する。

図２は、本発明の乱数発生装置の好ましい態様を示す構成図である。図２に示す乱数発生装置は、順次に接続された、スイッチング回路３０、発振回路４０、Ａ／Ｄ変換器５０、及びパーソナルコンピュータ６０を具えている。また、スイッチング回路３０には直流電源１０及び発振器２０が接続されている。

【００１２】

図３は、スイッチング回路３０の回路図の一例を示すものであり、直流電源１０より入力された直流の電源信号は、発振器２０から入力された矩形波によって変調を受け、矩形波状の電源信号が発振回路４０に向けて出力される。

【００１３】

図４は、アナログ発振回路４０の回路図の一例を示すものであり、スイッチング回路３０から前記矩形波状の電源信号が入力され、電気的信号として断続的に発振される。

【００１４】

発振回路４０より発振された電気的信号はＡ／Ｄ変換器５０に入力され、前記電気的信号はその振幅の大きさに応じてディジタルの電圧成分に変換される。次いで、前記ディジタルの電圧成分は、パーソナルコンピュータ６０に入力される。パーソナルコンピュータ６０には、前記ディジタル電圧成分に対する閾値が設定されており、次いで前記ディジタル電圧成分と前記閾値との大小関係が判別され、０又は１の数値が割り当てられる。

【００１５】

発振回路４０からの発振の初期、すなわち発振開始から定常状態に至るまでの立上り期間内においては、発振回路４０などのランダムな雑音の影響を受け、発振された電気的信号の周波数及び振幅は図１に示すように不安定となる。

したがって、この立上り期間内の電気的信号のみを採用し、上述した演算処理を

施することによって、０又は１の２進数的な乱数を発生することができる。

【００１６】

図５は、本発明の方法を用いて乱数を発生させる原理をモデル的に示したものである。図５に示すように、閾値よりも大きなディジタル電圧成分に対して１を割り当て、閾値よりも小さいディジタル電圧成分に対して０を割り当てることにより、０又は１の２進数からなる乱数を発生できることが分かる。

【００１７】

なお、本発明において、スイッチング回路３０は必須ではないが、スイッチング回路３０を設けることによって、上述した矩形波状の電源信号を発振回路４０内に導入することができ、直流電源１０を連続的にオンオフした際の電源信号を導入した場合と同様の効果を得ることができる。したがって、発振回路４０の立上り期間内におけるランダムな発振状態を簡易に生成できるようになる。

【００１８】

また、本発明においては、Ａ／Ｄ変換器５０に入力する際の前記電気的信号の周波数をサンプリング周波数よりも高いことが好ましい。前記電気的信号の周波数が前記サンプリング周波数以下となってしまうと、例えば、Ａ／Ｄ変換器５０からは図６に示すようなディジタル電圧成分が出力されてしまう場合がある。この場合に、上述したように０又は１を割り当てても、０又は１の数値が連続して出現するようになってしまい、目的とする乱数を発生することができない場合がある。

【００１９】

サンプリング周波数が高いほど乱数を高速で発生できるようになるので、図３に示す発振回路４０におけるキャパシタ及びコイルの値を適宜に設定して、より高い周波数の電気的信号を発生することにより、上記関係を満足し、２進数的な乱数を高速かつ安定的に発生することができる。

【００２０】

以上、具体例を挙げながら発明の実施の形態に基づいて本発明を詳細に説明してきたが、本発明は上記内容に限定されるものではなく、本発明の範疇を逸脱しない限りにおいて、あらゆる変形や変更が可能である。例えば、矩形波状の電源

信号を得るべく、図３に示すようなスイッチング回路３０を用いたが、その他の公知の手段によって前記矩形波状の電源信号を得ることができる。また、電気的信号の発振手段として図４に示す発振回路を用いたが、その他の手段を用いて前記電気的信号を発振させることもできる。

【００２１】

例えば、上述したアナログ発振回路の代わりにディジタル発振回路を用いることもできる。図７は、非安定性マルチバイブレータ型の発振回路４０の一回路図を示すものである。図７に示す非安定製マルチバイブレータ発振回路４０に対して、スイッチング回路３０から矩形波電圧が印加されると、発振回路４０からは断続的な発振が生成される。したがって、前記発振に基づく出力電圧（電気的信号）を出力側から取り出し、上述したようなＡ／Ｄ変換器５０を介してパーソナルコンピュータ６０に導入し、上述した演算処理を施すことによって、乱数を得ることができる。

【００２２】

なお、二組の非安定性マルチバイブレータを用い、一方のマルチバイブレータをスイッチング回路として用い、他方を上述した発振回路として用いることもできる。この場合、スイッチング回路と発振回路とを同一チップとして作製することができ、パーソナルコンピュータ６０内などの簡易に組み込むことができる。

【００２３】

図８は、ディジタルＩＣを用いたＬＣ発振回路４０の一回路図を示すものである。図８に示す発振回路４０は４段のディジタルＩＣを有しており、左側のＩＣ１～ＩＣ３はＡＮＤ回路の入力がショートされ、正帰還のＬＣ回路を構成する。スイッチング回路３０から矩形波電圧が印加されると、発振回路４０からは断続的な発振が生成される。右側のＩＣ４におけるＡＮＤはバッファであって、発振回路４０からの発振に起因する出力電圧（電気的信号）をＩＣ４から取り出す。その後、前記出力電圧に起因した電気的信号をＡ／Ｄ変換器５０を介してパーソナルコンピュータ６０に導入し、上述した演算処理を施すことによって、乱数を得ることができる。

【００２４】

なお、図８に示すディジタルＩＣを含む発振回路を用いる場合、トランジスタなどを使用しないので、図７に示す非安定性マルチバイブレータ発振回路に比べて低コスト化することができる。

【００２５】

図７及び図８に示すようなディジタル発振回路４０を用いる場合は、Ａ／Ｄ変換器５０を用いることなく、前記発振回路の出力電圧に起因した電気的信号を直接パーソナルコンピュータ６０に導入することもできる。また、図７及び図８に示すディジタル発振回路４０中にダイオードを追加し、発振波形の立ち上がりを向上させることもできる。

【００２６】

【発明の効果】

以上説明したように、本発明によれば、廉価かつ簡易な構成の装置を用いて、より無秩序な乱数を発生させる新規な方法、並びに前記方法に適用する装置を提供することができる。

【図面の簡単な説明】

【図１】　本発明の乱数発生方法の原理を説明するための図である。

【図２】　本発明の乱数発生装置の好ましい態様を示す構成図である。

【図３】　スイッチング回路の回路図の一例である。

【図４】　発振回路の回路図の一例である。

【図５】　本発明の方法を用いて乱数を発生させる原理をモデル的に示した図である。

【図６】　本発明の方法において、乱数が発生されない場合の原理をモデル的に示した図である。

【図７】　発振回路の回路図の他の例である。

【図８】　発振回路の回路図のその他の例である。

【符号の説明】

１０　直流電源

２０　発振器

３０　スイッチング回路

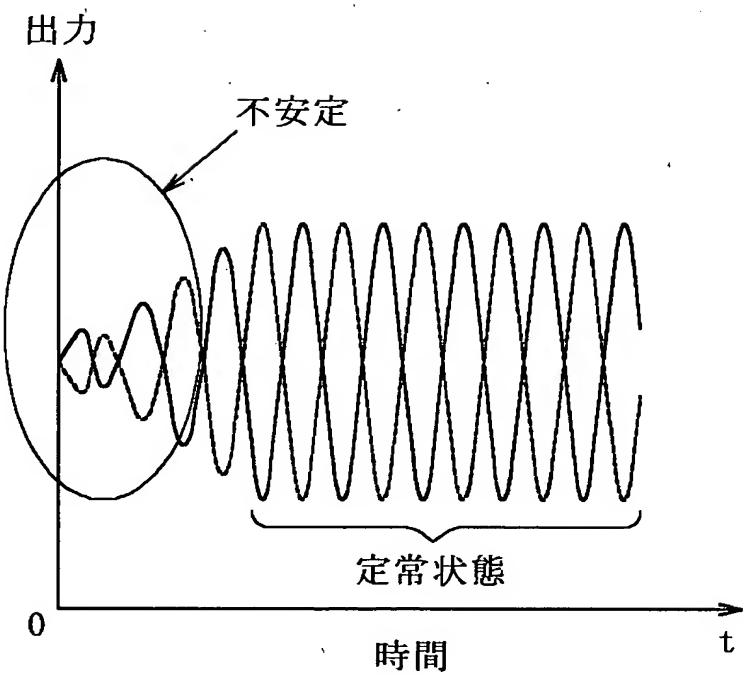
４０　発振回路

５０　Ａ／Ｄ変換器

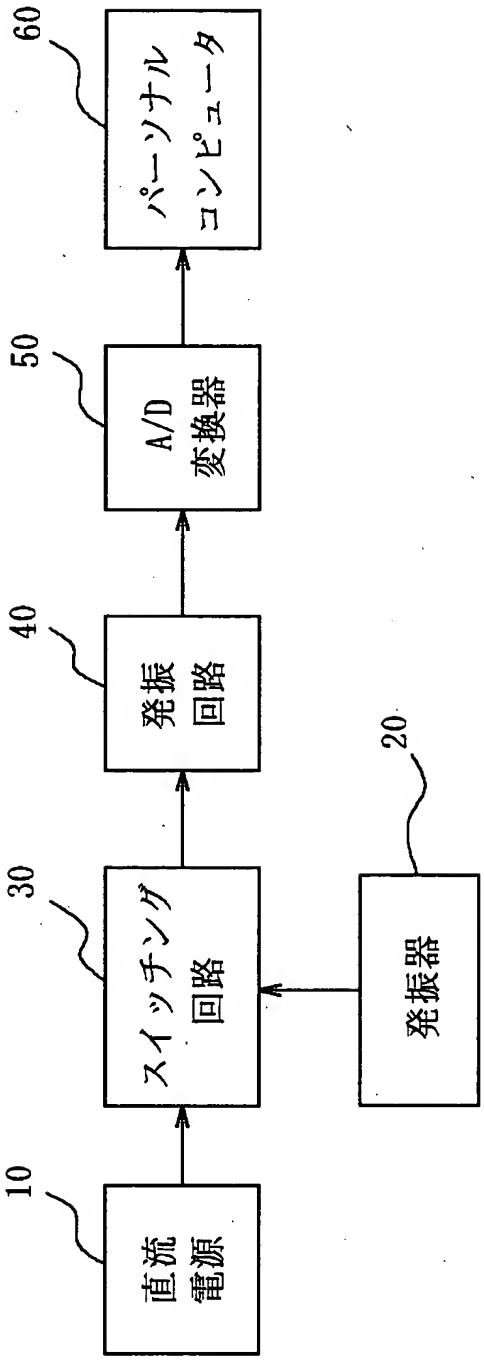
６０　パーソナルコンピュータ

【書類名】　　図面

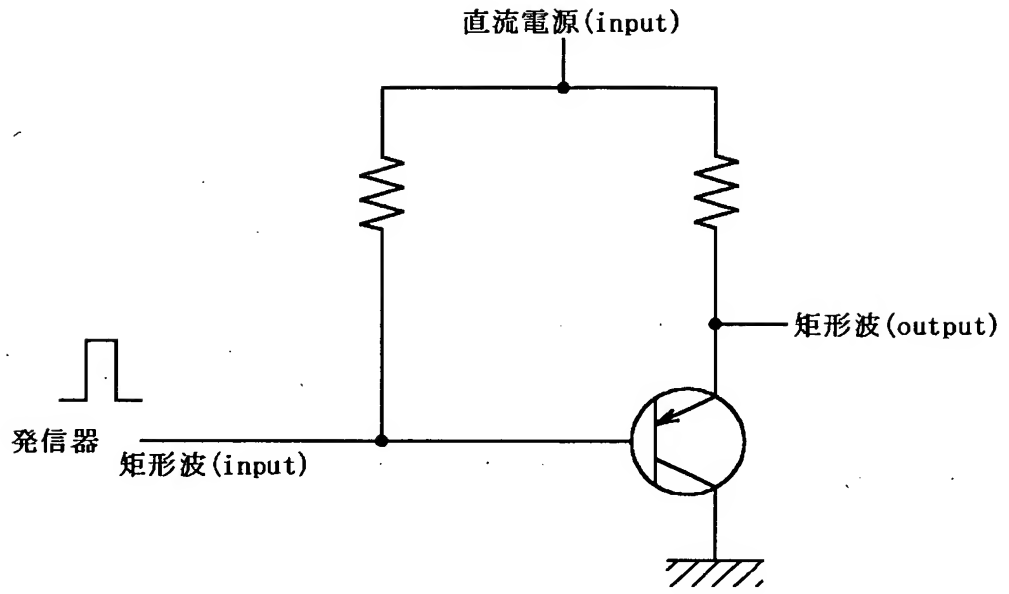
【図１】



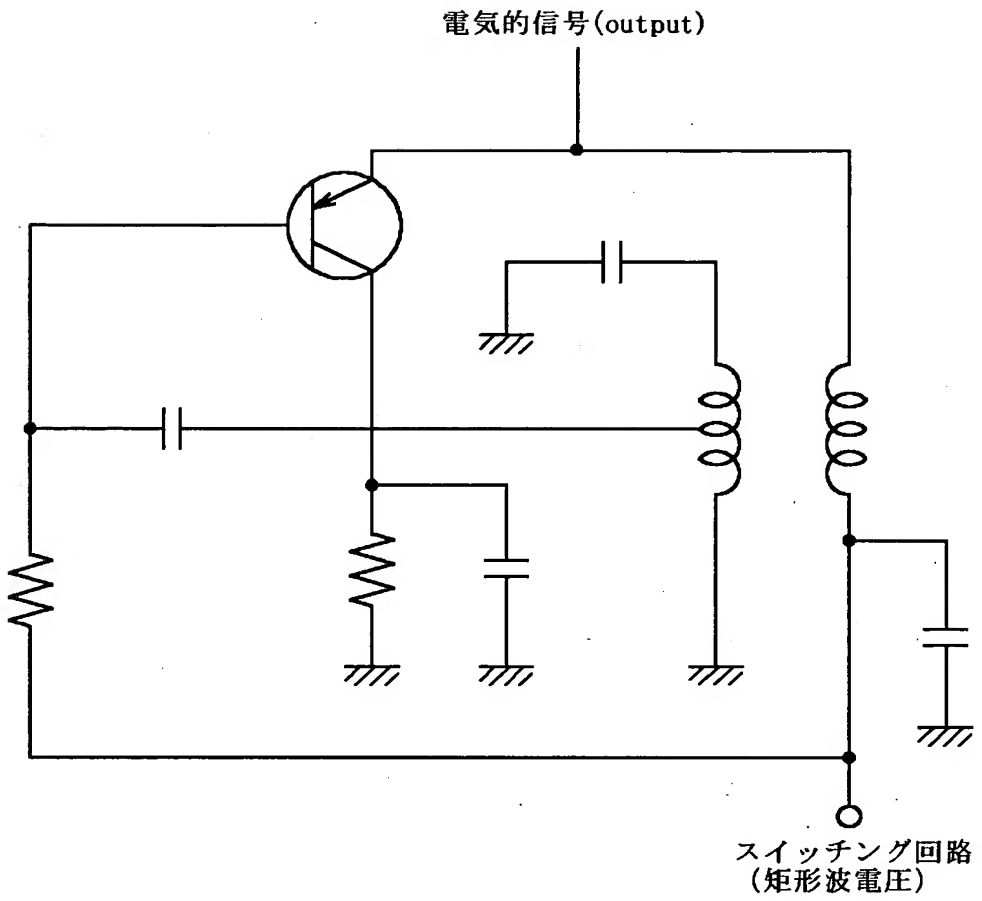
【図２】



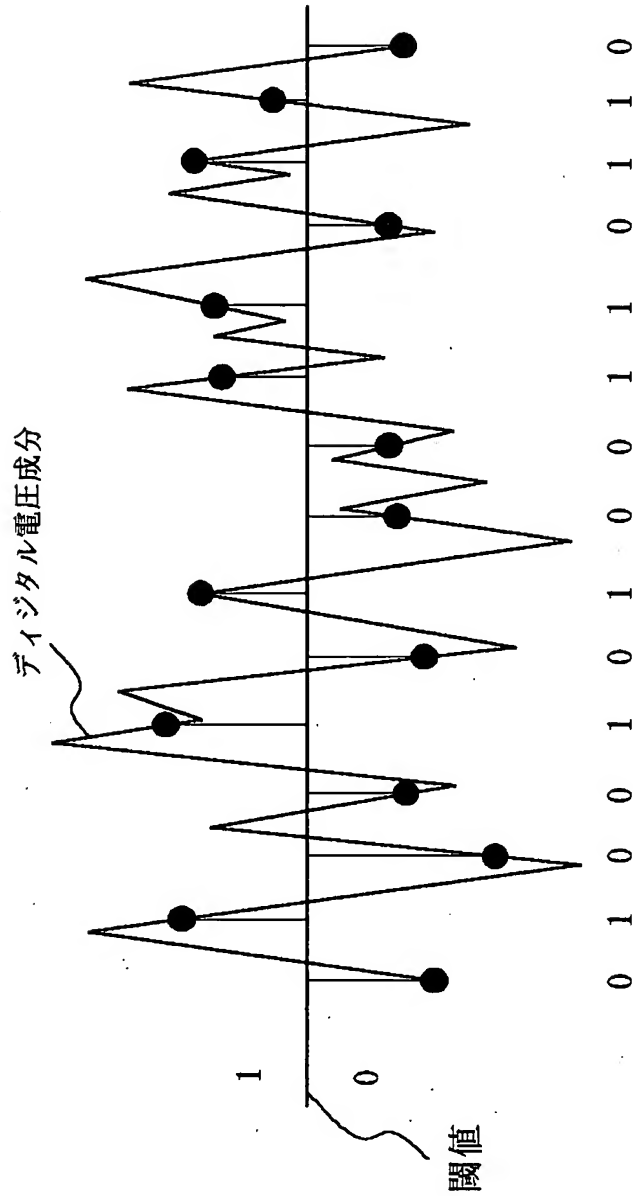
【図３】



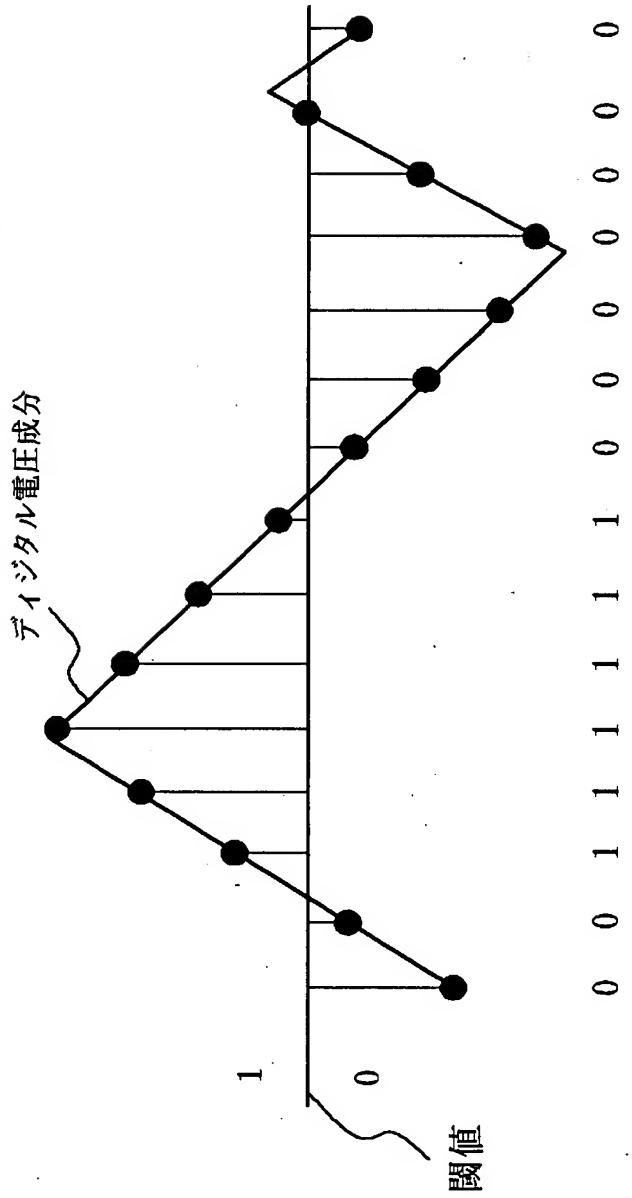
【図４】



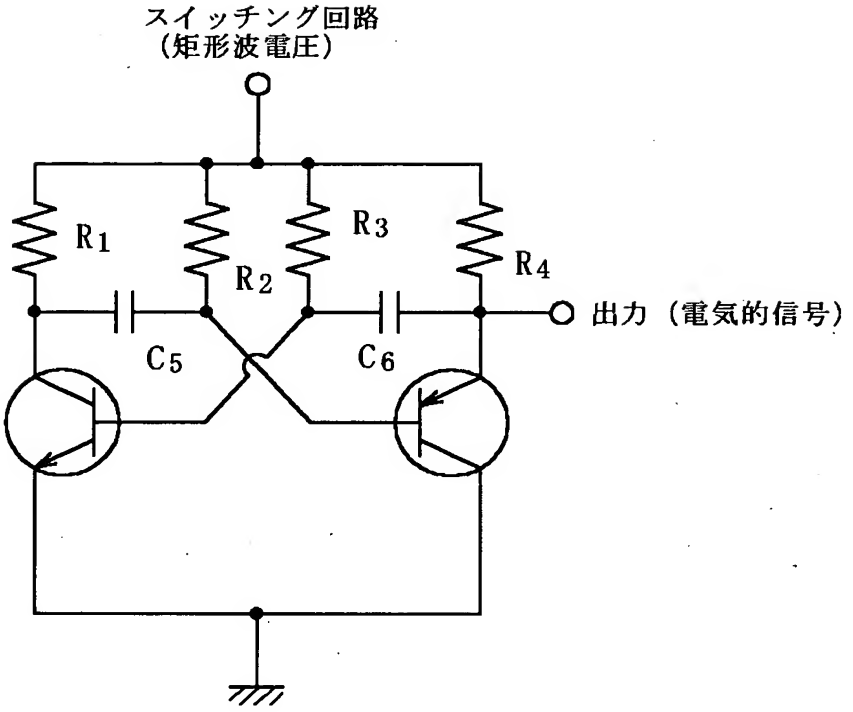
【図５】



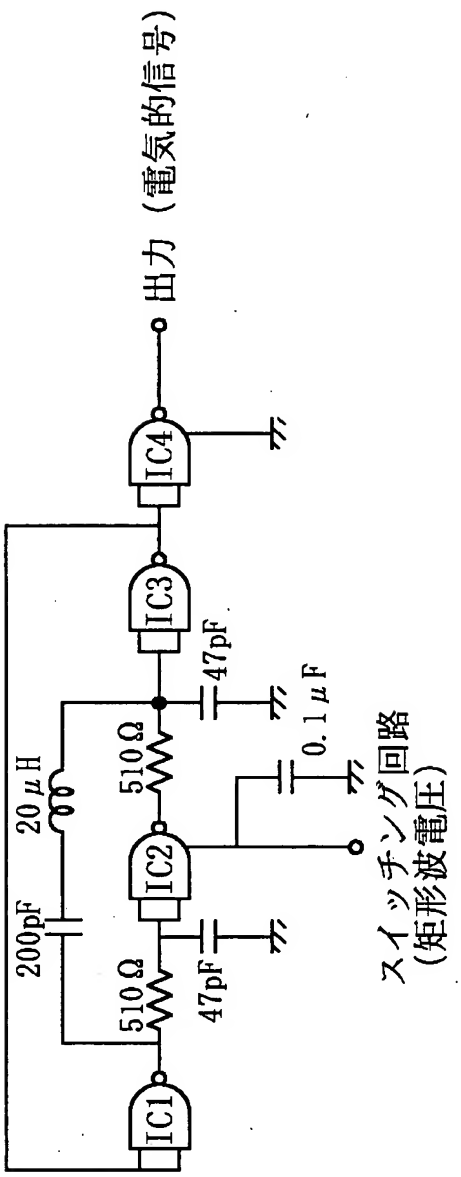
【図６】



【図７】



【図８】


出力（電気的信号）
IC4
IC3
IC2
IC1
47pF
0.1μF
510Ω
20μH
200pF
510Ω
47pF
スイッチング回路
（矩形波電圧）

【書類名】　　要約書

【要約】

【課題】　廉価かつ簡易な構成の装置を用いて、より無秩序な乱数を発生させる新規な方法、並びに前記方法に適用する装置を提供する。

【解決手段】　発振開始から定常状態に至るまでの立上り期間内において、発振回路４０より発振された電気的信号をＡ／Ｄ変換器５０に入力し、前記電気的信号をその振幅の大きさに応じてディジタルの電圧成分に変換する。次いで、前記ディジタル電圧成分を、パーソナルコンピュータ６０に入力する。パーソナルコンピュータ６０には、前記ディジタル電圧成分に対する閾値が設定されており、前記ディジタル電圧成分と前記閾値との大小関係が判別され、０又は１の数値が割り当てられ、２進数的な乱数を発生する。

【選択図】　　図５

認定・付加情報

特許出願の番号	特願２００２－３２３７９４
受付番号	５０２０１６８２９６０
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１４年１１月１２日

＜認定情報・付加情報＞

【特許出願人】

【識別番号】	596133441
【住所又は居所】	新潟県新潟市五十嵐２の町８０５０番地
【氏名又は名称】	新潟大学長

【代理人】　申請人

【識別番号】	100072051
【住所又は居所】	東京都千代田区霞が関３－２－４　霞山ビル７階
【氏名又は名称】	杉村　興作

【選任した代理人】

【識別番号】	100059258
【住所又は居所】	東京都千代田区霞が関３－２－４　霞山ビル７階
【氏名又は名称】	杉村　暁秀

次頁無

出　願　人　履　歴　情　報

識別番号　　〔５９６１３３４４１〕

１．変更年月日　　１９９６年　９月１１日
［変更理由］　新規登録
住　所　　新潟県新潟市五十嵐２の町８０５０番地
氏　名　　新潟大学長